# **Introduction**

**PROJECT Intro, Aim, scope, objective of Identifying Potential Vulnerabilities in a generic Android based Infotainment Systems Emulated within Android Studio**

This report will identify the privacy risks in the Honda Android Automotive OS Emulator by researching and identifying what type of documents are identified in the privacy policy and permissions in daily applications. It will detail the types of information collected and how the information in question is being used. There will also be an assessment of the privacy policies of the commonly used apps, namely: Maps, Google Play Services, and Location. The report manually tests the permissions of possible privacy risks and matches the findings against industry best practices and legal requirements, such as GDPR, in order to make recommendations on how to better manage users' data securely and in compliance with the law concerning connected automotive systems.

## Problem Description, Context and Motivation

What this research tried to answer is basically the grave risks of privacy and data security associated with app permissions in the Honda Android Automotive OS. Also, the role of most common programs, which require a great number of permissions for good functionality, is pointed out, such as Google Play Services, Maps, and Location. For example, Google Play Services would want access to Call Logs, Physical Activity, and others, while Maps would request Camera, Contacts, Location, etc. Pressing "Allow only while in use" or even "Deny" to limit those permissions could potentially get users blocked by the system, warning of an inability for these features to work anymore-a kind but blunt way to push users into giving full access.

These are issues of concern for both the users and the OEMs/Tier 1 suppliers of the infotainment systems, since constant collection of private user data might be used in the wrong direction. In this regard, the problem is that the car's infotainment system is used all the time; therefore, it is omnipresent and unavoidable. This is something that needs to be addressed in order for users to interact with such systems without putting themselves in some sort of safety and personal data risk. The presented study will assess those risks against the industry standards and regulatory obligations, such as GDPR, and will make recommendations on ways to enhance privacy safeguards within the connected car environment.

## 

## Aims

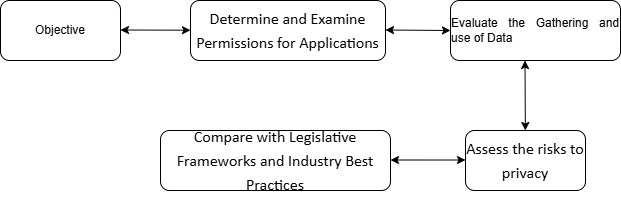
This project addresses three major objectives that are planned to be achieved in the context of Privacy and Data Security in Honda's Android Automotive Operating System.

1. Identify and Document Privacy Risks: Enumerate and document privacy risks of permissions for applications running on Honda Android OS. The report targets the research of typical applications like Maps, Location, and Google Play Services.
2. Evaluate Data Collection and Usage: Scrutinize how these applications collect and make use of data that is sensitive while comparing the findings with industry norms and legal frameworks like GDPR.
3. Develop Recommendations for Privacy Enhancements: The ultimate objective is the delivery of actionable recommendations toward the mitigation of identified privacy risks. This shall include recommendations on how to enhance the permission handling and user data security related to the infotainment system, taking into consideration compliance issues with regulatory standards, apart from growing user trust in the security or privacy measures of the infotainment system.

## Objectives

The goals of the project comprise the assessment and enhancement of privacy features on Honda's Android Automotive OS. In particular, this is an application that comprises very important applications such as Google Play Services, Maps, and Location. Subsequent actions will be performed as described to address these objectives:

**Figure 1**



1. **Determine and Examine Permissions for Applications:** The various kinds of permissions which fall under categories such as Allow Always, Allow only when the app is at work, and denied are to be identified in the case of Maps, Location, and Google play service apps.
2. **Evaluate the Gathering and use of Data:** Investigate the 3 types of data collected, including Allow all the time, Allow only the app in use, and denied, including Google play service Call Logs, Camera, Contacts, Files and Media, Location, Microphone, Phone, Physical Activity, SMS, Car Information for Maps, Camera, contacts, files, and Media, Location, Microphone, Physical Activity, and car information. Following that, evaluate how this information is used, paying specific attention to privacy implications.
3. **Assess the risks to Privacy:** Analyze the potential privacy risks that could be associated with such permissions in automotive infotainment, considering consequences including data misuse, unauthorized access, and security breaches in relation to automobiles.
4. **Compare with Legislative Frameworks and Industry Best Practices:** Analyze the privacy policies in terms of the best practices and industry standards, like GDPR, and regulatory frameworks in order to check for compliance and advise on future improvements to be considered in user privacy and data security within Honda's car infotainment systems.

## Legal

The project will explain the legal implications related to privacy and data security of Honda's Android Automotive OS. Some of the major legal considerations are discussed here, including legal risks, consent and permission, GDPR compliance, data security measures, and data protection laws. The project will be based on data usage and permissions in Honda's Android Automotive OS with a view to claiming compliance status under regulatory frameworks such as the GDPR. It is mainly about the mitigation of risk of compliance, user data protection from legal liabilities, and assurance that privacy policies and practices comply with regulatory requirements.

## Social

From social points of view regarding this project, the considerations are directed to the wider impacts, both on the users and society as a whole:

User privacy and trust, where it shows how it impacts the user experience, data sensitivity, accountability, and transparency and social responsibility. The project emphasizes user trust and security of data in relation to the impact of data privacy on Honda's Android Automotive OS. This study shall seek to protect the personal information of the users and contribute to a more secure and responsible usage of automotive infotainment systems by spotting the risks while increasing the safeguards of privacy.

## Ethical

Therefore, the project will address the ethical issues in evaluating the impact that different data collections and permission practices have on user privacy. This is to ensure that Honda's Android Automotive OS follows ethical standards, respects user autonomy, and does not result in any possible misuses so as to promote transparency and accountability.

This will be a project in which ethical considerations are going to be central. It is supposed to address the moral implications of data privacy practices.

Respect for User Autonomy, Data Minimisation, Transparency and Honesty, Prevention of Data Abuse, Balancing Use and Privacy

## Professional

The project will be done in accord with severe professional standards to make sure that it is both accurate and ethical. Principal considerations would involve thorough privacy risk analysis regarding data practice, compliance with industry best practice and legal standards like GDPR, and acquisition of ethical clearances. It ensures transparency in reporting and impartial recommendations, maintaining professional integrity with confidentiality. The stakeholders' involvement and feedback would make the findings relevant and effective. Risk management strategies would address potential data security issues, and the project's outcomes would be credible and actionable, according to the industry norm and ethical standards of best practice.

Next, addressing these professional considerations, the project will seek to ensure that its output is in the form of credible, actionable, and ethical recommendations on how best to enhance privacy and data security in Honda's Android Automotive OS.

## Background

The project discusses manual testing of the application in Honda Android Automotive OS Emulator, given that it performs nondisclosure of data regarding car owners. In actual sense, such testing is very important because it allows for the identification of privacy and permission risks that might compromise user security and make cars unsalable if these aspects are not checked. Such a discussion has relevance in the automotive, where user data protection plays a prime role in everyday activities. The following project will implement a system that avoids data risks, considering the existing literature in automotive infotainment vulnerabilities and privacy concerns, making compliance with legal standards such as GDPR. Thus, the vehicles will be more trustable with increased safety.

## Report overview

This report is structured to analyze privacy and permission risks in the Honda Android Automotive OS applications such as Map, Location, and Google play services. It begins with the **Literature and Technology Review** - to find out which is the state of art on the issue of privacy and permission risks or vulnerabilities in apps for automotive systems, with an emphasis on those running on ANDROID-based platforms. **Methodology**- enumerates the procedures employed in analyzing permissions and privacy policies of applications in Honda Android Automotive OS Emulator. Further, **Implementation**-describes how these methodologies have been applied by installing the emulator and carrying out manual testing of each app's testing. **Evaluation and Results** critically evaluate findings that lead to a **Conclusion** summarizing the outcomes, proposing further work, and reflecting on the project. The report concludes with **References** and Appendices for further information.